HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

AF IFW

PATENT APPLICATION

ATTORNEY DOCKET NO. 10006270-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): John Patrick McGregor, Jr.

Confirmation No.:

Application No.: 10/001,682

Examiner: David G. Cervetti

Filing Date: 10/25/2001

Group Art Unit: 2136

Title: METHOD OF IMPLEMENTING THE DATA ENCRYPTION STANDARD WITH REDUCED COMPUTATION

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 02/07/2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

(X) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

(X)	one month	$120.00
( )	two months	$450.00
( )	three months	$1020.00
( )	four months	$1590.00

( ) The extension fee has already been filled in this application.

( ) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account **08-2025** the sum of **$620.00**. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

( ) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit: April 25, 2006

OR

( ) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number________ on ________

Number of pages:

Typed Name: Joanne Bourguignon

Signature: Joanne Bourguignon

Respectfully submitted,

John Patrick McGregor, Jr.

By

Robert W. Bergstrom

Attorney/Agent for Applicant(s)
Reg. No. **39,906**

Date: **April 25, 2006**

Telephone No.: **206.621.1933**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Applicant:	John Patrick McGregor, Jr.
Application No.:	10/001,682
Filed:	October 25, 2001
Title:	Method of Implementing the Data Encryption Standard with Reduced Computation

Examiner:	David G. Cervetti
Art Unit:	2136
Docket No.:	10006270-1
Date:	April 25, 2006

APPEAL BRIEF

Mail Stop: Appeal Briefs – Patents
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Examiner, in an Office Action mailed November 17, 2005, finally rejecting claims 1-19.

REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

Applicant's representative has not identified, and does not know of, any other appeals of interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-19 are pending in the application. Claims 1-19 were finally rejected in the Office Action dated November 17, 2005. Applicant's appeal the final rejection of claims 1-19, which are copied in the attached CLAIMS APPENDIX.

STATUS OF AMENDMENTS

No Amendment After Final is enclosed with this brief. The last Amendment was filed August 4, 2005.

SUMMARY OF CLAIMED SUBJECT MATTER

Overview

Embodiments of the present invention are directed to reducing the computational overhead for each round of the Data Encryption Standard ("DES") encryption and decryption method by reducing the number of instructions required to compute inputs, or indexes, to DES SP-boxes. The DES encryption method is described in detail in the current application with reference to Figures 1-4. The DES encryption method, as shown in Figure 1, generates an encrypted 64-bit block *C* from a 64-bit plain-text block *P* and a 56-bit encryption key *K*. The DES encryption method is applied, block-by-block, to successive 64-bit blocks of a plain-text data object in order to generate corresponding, identically sized, encrypted blocks that are assembled to produce an encrypted data object. The encryption of a 64-bit plain text block *P* is described, beginning on line 11 of page 2 of the current application, with reference to Figures 3-4. The plain-text block *P* is first permuted by an initial permutation step to generate a permuted 64-bit block. The permuted, 64-bit block is then subjected to 16 rounds of DES permutation-and-substitution operations. Following the 16 rounds of permutation-and-substitution operations, the 64-bit block is then again permuted in a final permutation operation to generate the 64-bit encrypted block *C*.

Figure 4 shows the steps undertaken in each of the 16 rounds of DES permutation-and-substitution operations. In each of the 16 permutation-and-substitution operations, a 64-bit intermediate block, generated either from the initial permutation step or a previous permutation-and-substitution round, is split into a left-hand 32-bit portion *L* and a right-hand 32-bit portion *R*. The right-hand portion *R* is first expanded and permuted from 32 bits to 48 bits in an expansion permutation operation, as discussed in lines 22-24 of page 2. Next, the 48-bit output of the expansion permutation operation is XORed with the output of a round-key-generation function *F* which takes, as inputs, an integer *j* specifying the current round (i.e., *j* = 1, 2, 3, . . . 16) and the encryption key *K*. The output of this XOR operation is then input to an S-box substitution step by splitting up the 48-bit XOR-operation result into eight consecutive 6-bit fields, and then using the 6-bit fields as indexes into eight different S-box lookup tables in order to produce a 4-bit result from each 6-bit S-box-table input. Thus, as a result of S-box substitution step, the 48-bit result from the XOR operation is contracted to a 32-bit result. This 32-bit result is then subject to a P-box permutation which permutes the 32-bit result to a different, permuted 32-bit result. The permuted 32-bit result is then XORed with the left-hand 32-bit portion *L* to produce a 32-bit right portion of the result of the current permutation-and-substitution operation, or round. The 32-bit right-hand portion *R* input to the current permutation-and-substitution operation is copied into the 32-bit left-hand portion of the result the current permutation-and-substitution operation, or round.

The above-discussed description of the DES encryption method provided in the current application is confirmed by Menezes et al., NPL Handbook of Applied Cryptography, pgs. 252-256 ("Menezes"), cited by the Examiner in rejecting claims 5-7 and 14-16. On pages 252-253, Menezes exactly and concisely describes the DES encryption method, including the above-discussed expansion permutation operation (step (a) in section 3 on page 253), XOR operation (step (b) in section 3 on page 253); S-box substitution step (step (c) in section 3 on page 253); and final 32-bit-to-32-bit permutation (step (d) in section 3 on page 253).

As discussed in the current application beginning on line 4 of page 4, it is possible to combine the S-box lookup table with the P-box permutation step by constructing combined SP-box lookup tables. SP-box lookup tables produce 32-bit results based on 6-bit inputs. Twenty-eight of these bits are set to zeros. Using SP-box lookup tables decreases the number of bit-manipulation operations needed to be executed in software, and thus increases the computational efficiency of DES encryption. An example shown on page 7 of the current application illustrates computation of a 12-bit SP-box index for a second large SP-box, as discussed in the current application beginning on line 17 of page 6, from a portion of the input *R* and a portion of the current round key generated by round-key-generation function *F*. As shown on page 7, the result of the expansion permutation operation followed by XOR of that result with the result produced by the round-key-generation function can be carried out in a single XOR operation between the 32-bit right portion of the input *R* and bits of the encryption key *K*. Examining the sequence of bits taken from the 32-bit input *R*, shown at approximately line 15 on page 7, it can be seen that these bits, specified by subscripted "x" characters, are not in sequential order. Specifically, the bit-pair x_{12} and x_{13} occurs twice, at positions 5 and 6 and at positions 7 and 8. These out-of-sequence bits require significant computational overhead to extract from *R* and reorder.

In embodiments of the present invention, as discussed beginning on line 7 of page 10, a different, ordered sequence of bits is chosen from *R*. These bits do not include the redundant occurrence of the bit pair x_{12} and x_{13} that occurs in the sequence used by the standard DES technique shown on approximately line 15 of page 7. The redundant occurrence of bits x_{12} and x_{13} is removed, shortening the sequence of bits extracted from *R*, and two zero bits are placed at the end of the 12-bit string to fill the 12-bit string. In addition, the bits chosen from the encryption key *K* are different from those chosen in the standard DES example of page 7, with two bit-wise XOR products included in the last two entries of the 12-bit portion of the encryption key shown on approximately line 15 of page 10. As discussed in the remaining lines of page 10, the information content of the two 12-bit strings shown on page 10 is equivalent to that of the two 12-bit strings shown on approximately lines 15 and 18 of page 7. However, all of the bits selected from the intermediate result *R* in the pair of 12-bit strings shown on Figure 10 are consecutively ordered, eliminating the need for expensive bit extraction and reordering operations. Standard DES permutation-and-substitution-operation results are obtained by re-ordering the SP-box entries, as discussed in the first paragraph of page 11.

Embodiments of the present invention decrease the number of assembler instructions, or high-level programming instructions, needed to carry out DES encryption. Thus, in standard DES encryption, pseudo assembly code for computing the 12-bit large-SP-box index is shown on lines 9-15 of page 8, while a much shorter pseudo assembly code, shown on lines 20-24 of page 14, is possible when reordering of input bits, modified *K* bits, and reordering of large SP-box entries, which together represents one embodiment of the present invention, is used. Because DES encryption rounds are performed a huge number of times, elimination of even three out of seven instructions within an inner loop of the DES encryption process may represent significant computational savings. It needs to be emphasized that, as claimed in each of the independent claims of the current application, the present invention is directed to a method and system for performing standard DES encryption more computationally efficiently.

Independent Claims 1 - 2

Claim 1 is directed to a method for reducing computation during each Data Encryption Standard (DES) encryption and decryption round by (1) generating at least one large SP-box lookup table; (2) computing an index for each SP-box lookup table; (3) adding operations to the DES round key computation function to obtain a modified round key computation function; and (4) computing the index for each SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES expansion permutation and the modified round key computation function. SP-boxes and SP-box lookup tables are discussed on lines 4-15 of page 4 of the current application. Background for that discussion begins on line 11 of page 2 and continues to line 4 of page 4. Adding of operations to the DES round key computation in order to facilitate less computationally expensive SP-box indexing is discussed on lines 7-17 of page 11 of the current application. Computing an index for a large SP-box is shown diagrammatically in the XOR operations between bit strings provided on page 7 and page 10 of the current application, and in Figures 5-8. In the bit-string XOR operation shown on lines 11-15 of page 10, a 12-bit large SP-box input or index is computed using a single block of contiguous bits from the right-hand input *R*. The standard DES encryption technique is illustrated in Figures 1-4 of the current application.

Independent claim 2 is directed to reducing the number of software instructions required to perform permutation-and-substitution operations using Data Encryption Standard (DES) encryption and decryption rounds, wherein each round has a 64-bit input, and 32 bits of that 64-bit input are applied as the input to the DES Expansion Permutation, by: (1) generating at least one large SP-box lookup table; (2) adding operations to the DES round key computation function to obtain a modified round key computation function; (3) computing a modified SP-box index by performing XOR operations between at least one block of contiguous bits of the 32-bit input to the DES Expansion Permutation and the result of the modified round key computation function; and (4) executing each subsequent round of DES computation by repeating steps (1) and (3). SP-boxes and SP-box lookup tables are discussed on lines 4-15 of page 4 of the current application. Background for that discussion begins on line 11 of page 2 and continues to line 4 of page 4. Adding of operations to the DES round key computation in order to facilitate less computationally expensive SP-box indexing is discussed on lines 7-17 of page 11 of the current application. Computing an index for a large SP-box is shown diagrammatically in the XOR operations between bit strings provided on page 7 and page 10 of the current application, and in Figures 5-8. In the bit-string XOR operation shown on lines 11-15 of page 10, a 12-bit large SP-box input or index is computed using a single block of contiguous bits from the right-hand input *R*. The standard DES encryption technique is illustrated in Figures 1-4 of the current application.

Dependent Claims 3 – 7

Claim 3 is directed to the method of claim 2 carried out in a digital processor. Claim 4 elaborates on various types of digital processors mentioned in claim 3. Claim 5 further expands the third step of claim 2 to include selecting two blocks of contiguous bits for computing a modified SP-box index. Claim 6 further specifies the positions of the least significant and most significant bits of the 32-bit input within the two selected blocks. Claim 7 specifies a permutation of the entries of each SP-box lookup table, as discussed on lines 1-6 of page 11 of the current application.

Independent Claim 8

Claim 8 is directed to a method of reducing computation associated with the DES Expansion Permutation, in a processor carrying out a Data Encryption Standard (DES) computation by iterative DES rounds, by reducing the number of instructions required to compute the inputs to DES SP-boxes by: (1) mathematically transforming the DES round function in each said round; (2) mathematically transforming the DES round key computation function in each said round; and (3) modifying the inputs to said SP-boxes in accordance with the results of steps (1) and (2). SP-boxes and SP-box lookup tables are discussed on lines 4-15 of page 4 of the current application. Background for that discussion begins on line 11 of page 2 and continues to line 4 of page 4. Transforming the DES round key computation in order to facilitate less computationally expensive SP-box indexing is discussed on lines 7-17 of page 11 of the current application. The standard DES encryption technique is illustrated in Figures 1-4 of the current application.

Dependent Claim 9

Claim 9 further specifies that the first two steps of claim 8 are carried out by shifting them from DES expansion permutation step to the DES round key computation function, as discussed in the current application beginning on line 18 of page 13.

Independent Claims 10 – 11

Claim 10 is directed to an apparatus for reducing computation during each Data Encryption Standard (DES) encryption and decryption round, the apparatus comprising (1) means for generating at least one large SP-box lookup table; (2) means for computing an index for each SP-box lookup table; (3) means for adding operations to the DES round key computation function to obtain a modified round key computation function; and (4) means for computing the index for each said SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and the modified round key computation function. SP-boxes and SP-box lookup tables are discussed on lines 4-15 of page 4 of the current application. Background for that discussion begins on line 11 of page 2 and continues to line 4 of page 4. Adding of operations to the DES round key computation in order to facilitate less computationally expensive SP-box indexing is discussed on lines 7-17 of page 11 of the current application. Computing an index for a large SP-box is shown diagrammatically in the XOR operations between bit strings provided on page 7 and page 10 of the current application, and in Figures 5-8. In the bit-string XOR operation shown on lines 11-15 of page 10, a 12-bit large SP-box input or index is computed using a single block of contiguous bits from the right-hand input *R*. The standard DES encryption technique is illustrated in Figures 1-4 of the current application.

Claim 11 is directed to an apparatus for reducing the number of software instructions required to perform permutation-and-substitution operations in the Data Encryption Standard (DES) encryption and decryption rounds, wherein each round has a 64-bit input and 32 bits of that 64-bit input are applied as the input to the DES Expansion Permutation, the apparatus comprising (1) means for generating at least one large SP-box lookup table; (2) means for adding operations to the DES round key computation function to obtain a modified round key computation function; and (3) means for computing a modified

SP-box index by performing XOR operations between at least one selected block of said 32-bit input to the DES Expansion Permutation and the result of the modified round key computation function. SP-boxes and SP-box lookup tables are discussed on lines 4-15 of page 4 of the current application. Background for that discussion begins on line 11 of page 2 and continues to line 4 of page 4. Adding of operations to the DES round key computation in order to facilitate less computationally expensive SP-box indexing is discussed on lines 7-17 of page 11 of the current application. Computing an index for a large SP-box is shown diagrammatically in the XOR operations between bit strings provided on page 7 and page 10 of the current application, and in Figures 5-8. In the bit-string XOR operation shown on lines 11-15 of page 10, a 12-bit large SP-box input or index is computed using a single block of contiguous bits from the right-hand input *R*. The standard DES encryption technique is illustrated in Figures 1-4 of the current application.

Dependent Claims 12 – 16

Claim 12 is directed to the method of claim 11 carried out in a digital processor. Claim 13 elaborates on various types of digital processors mentioned in claim 12. Claim 14 further expands the third step of claim 11 to include selecting two blocks of contiguous bits for computing a modified SP-box index. Claim 15 further specifies the positions of the least significant and most significant bits of the 32-bit input within the two selected blocks. Claim 16 specifies a permutation of the entries of each SP-box lookup table, as discussed on lines 1-6 of page 11 of the current application.

Independent Claim 17

Claim 17 is directed to an apparatus for reducing computation associated with the DES Expansion Permutation by reducing the number of instructions required to compute the inputs to DES SP-boxes, the apparatus comprising (1) means for mathematically transforming the DES round function in each said round; (2) means for mathematically transforming the DES round key computation function in each said round; and (3) means for modifying the inputs to said SP-boxes in accordance with the transformations of said round function and of said round key computation function. SP-boxes and SP-box lookup tables are discussed on lines 4-15 of page 4 of the current application. Background for that discussion begins on line 11 of page 2 and continues to line 4 of page 4. Transforming the DES round key computation in order to facilitate less computationally expensive SP-box indexing is discussed on lines 7-17 of page 11 of the current application. The standard DES encryption technique is illustrated in Figures 1-4 of the current application.

Dependent Claim 18

Claim 18 further elaborates the method of claim 17, with the computation in the DES Expansion Permutation step shifted from the DES round function to the DES round key computation function.

Independent Claim 19

Claim 19 is directed to a data processing system for carrying out Data Encryption Standard (DES) encryption and decryption rounds with reduced computation, the system comprising (1) computer processing means for processing data; (2) storage means providing four large SP-box lookup tables; (3) means for computing indices for the respective SP-box lookup tables;(4) means for adding operations to the DES round key computation function to obtain a modified round key computation function; and (5) means for computing the index of each said SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function. SP-boxes and SP-box lookup tables are discussed on lines 4-15 of page 4 of the current application. Background for that discussion begins on line 11 of page 2 and continues to line 4 of page 4. Adding of operations to the DES round key computation in order to facilitate less computationally expensive SP-box indexing is discussed on lines 7-17 of page 11 of the current application. Computing an index for a large SP-box is shown diagrammatically in the XOR operations between bit strings provided on page 7 and page 10 of the current application, and in Figures 5-8. In the bit-string XOR operation shown on lines 11-15 of page 10, a 12-bit large SP-box input or index is computed using a single block of contiguous bits from the right-hand input *R*. The standard DES encryption technique is illustrated in Figures 1-4 of the current application.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Rejections of claims 1-3, 8-12, and 17-19 under 35 U.S.C. §102(b) as being anticipated by Adams et al., U.S. Patent No. 5,825,886 ("Adams").

2. Rejections of claims 4 and 13 under 35 U.S.C. §103(a) as being unpatentable over Adams in further view of Candelore, U.S. Patent No. 5,861,662.

3. Rejections of claims 5-7 and 14-16 under 35 U.S.C. §103(a) as being unpatentable over Adams in further view of Menezes et al., NPL Handbook of Applied Cryptography, pgs. 252-256.

ARGUMENT

Claims 1-19 are pending in the current application. In an Office Action dated November 7, 2005 ("Office Action"), the Examiner rejected claims 1-3, 8-12, and 17-19 under 35 U.S.C. §102(b) as being anticipated by Adams et al., U.S. Patent No. 5,825,886 ("Adams"), rejected claims 4 and 13 under 35 U.S.C. §103(a) as being unpatentable over Adams in view of Candelore, U.S. Patent No. 5,861,662 ("Candelore"), and rejected claims 5-7 and 14-16 under 35 U.S.C. §103(a) as being unpatentable over Adams in further view of Menezes et al., NPL Handbook of Applied Cryptography, pgs. 252-256 ("Menezes"). Applicant's representative respectfully traverse these 35 U.S.C. §102 and §103 rejections.

ISSUE 1

1. Whether claims 1-3, 8-12, and 17-19 are anticipated under 35 U.S.C. §102(b) by Adams.

First, Applicant's representative provides an overview of Adams, the primary reference employed in all of the 35 U.S.C. §102 and 35 U.S.C. §103 rejections made by the Examiner. As clearly stated in the Abstract and in the Field of the Invention sections of Adams, Adams discloses a "new design procedure for constructing a family of *DES-like* Substitution Permutation Network (SPN) cryptosystems with desirable cryptographic properties" (emphasis added). Adams' invention "resides generally in symmetric cryptosystems and their construction procedures. In particular, it is directed to *new ciphers* which belong to a family of DES-like substitution-permutation network cryptosystems and to *methods of cryptographically transforming plain text into cipher text using such novel ciphers*" (emphasis added). Thus, beginning immediately with the Abstract and Field of the Invention sections of Adams, it is clear that Adams is directed not to DES encryption, but to a new encryption system.

In the first portion of the Background of the Invention section of Adams, beginning on line 14 of column 1, Adams states:

> This invention relates to a design procedure for a family of symmetric encryption algorithms. The ciphers produced, known as CAST ciphers, are provably resistant to differential cryptanalysis, linear cryptanalysis, and related-key-cryptanalysis. Furthermore, they can be shown to posses a number of desirable cryptographic properties such as avalanche, Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), and an absence of weak and semi-weak keys. *CAST ciphers are based on the well-understood and extensively-analyzed framework of the Feistel cipher*—the framework used in DES—*but with a number of improvements (compared to DES) in both the round function and the key schedule which guarantee good cryptographic properties in fewer rounds than DES.* These ciphers therefore have very good encryption/decryption performance (comparing very favorably with many alternatives of similar cryptographic strength) and can be designed with parameters which make them particularly suitable for software implementations on 32-bit machines. (emphasis added)

Thus, Adams is directed to a family of encryption algorithms that employ CAST ciphers. CAST ciphers are, as clearly stated by Adams, different from the ciphers employed in the standard DES cryptography procedures, discussed further below.

Figure 1 of Adams, as discussed in Adams beginning on line 23 of column 2, illustrates the general Feistel-structured SPN on which CAST ciphers employed by Adams are based. Note that, by comparison to Figures 3 and 4 of the current application, the Feistel-structured SPN differs from the DES encryption method. For example, comparing Figure 1 of Adams to Figure 3 of the current application, the Feistel-structured SPN lacks the initial permutation and final permutation steps. Figure 2 of Adams shows a round function employed in the encryption method disclosed by Adams. This round function is shown in Figure 1 of Adams as blocks labeled F_1, F_2, . . . F_n. Comparing this round function of Adams, shown in Figure 2 of Adams, with the DES round function shown in Figure 4 of the current application, it is clear that Adams' system does not carry out a DES expansion permutation step, as in the DES encryption method shown in Figure 4 of the current application, and also does not carry out a P-box permutation step, also shown in Figure 4 of the current application. The function **a** in Figure 2 of Adams is, according to one embodiment of Adams, an XOR addition, as discussed beginning on line 35 of column 5 of Adams. Additional, more complex operations may also be used, according to Adams. However, Adams does not mention the expansion permutation step shown in Figure 4 of the current application and discussed in the current application on lines 22-24 of page 2 and shown in the current application in Table 1 on page 4. Figure 2 of Adams also does not include a P-box permutation, as shown in Figure 4 of the current application. As clearly shown in Figure 2 of Adams, all of the S-box-based operations generate 32-bit integers from two 32-bit arguments. However, as discussed above, the expansion permutation step, shown in Figure 4 of the current application, generates a 48-bit integer, and the S-box substitution step of Figure 4 of the current application ends up collapsing a 48-bit result of the XOR operation into 32 bits by generating 4-bit quantities from 6-bit indices. On lines 54-58 of column 2 of Adams, Adams explicitly states:

> The CAST design procedure makes use of substitution boxes which have fewer input bits than output bits (e.g., 8x32); this is the opposite of DES and many other ciphers which use s-boxes with more input bits than output bits (e.g., 6x4).

As discussed above, and as stated in the above-quoted portion of Adams, the standard DES encryption method employs substitution boxes with a greater number of input bits than output bits. Specifically, as discussed on lines 6-8 of page 3 of the current application, the DES encryption system inputs 6-bit indexes to S-box lookup tables to generate corresponding 4-bit results.

Thus, Adams' CAST-cipher based encryption method differs significantly from the standard DES encryption method discussed in the current application with reference to Figures 1-4. Specifically, Adams' CAST-cipher based encryption method does not employ the initial and final permutation steps, and does not employ, in each round, the DES expansion permutation operation, the DES S-box substitution step, and the final 32-bit-to-32-bit permutation. Therefore, Adams' CAST-cipher based encryption method does not employ DES S-boxes, P-boxes, and SP-boxes, since, as explicitly stated by Adams, Adams' method uses a different type of S-box, and Adams does not use, or mention or suggest the use of P-boxes and SP-boxes.

In the 35 U.S.C. §102(b) anticipation rejection of claim 1 by Adams, the Examiner states that Adams teaches "generating at least one large SP-box lookup table" on lines 23-34 of column 5. Lines 23-34 of column 5 are reproduced below, for the reader's convenience:

> Fig. 2 illustrates the round function according to one embodiment of the invention. This embodiment uses a 64-bit

> blocksize and 8x32 s-boxes. Referring to the figure, a 32-bit data half is input to the function along with a subkey K_i. These two quantities are combined using operation "a" and the 32-bit result is split into four 8-bit pieces. Each piece is input to a different 8x32 s-box (S_1, . . . S_4). S-boxes S_1 and S_2 are combined using operation "b"; the result is combined with S_3 using operation "c"; this second result is combined with S_4 using operation "d." The final 32-bit result is the output of the round function.

As the reader will quickly discern from the above-quoted section of Adams, there is not a single mention of SP-boxes, SP-box lookup tables, or generation of SP-box lookup tables in the cited portion of Adams. Instead, the cited portion of Adams describes the non-DES round function shown in Figure 2 of Adams, as discussed above. As discussed in the current application beginning on line 4 of page 4, SP boxes represent a combination of DES S-boxes and P-boxes. As discussed above, the P-box is a final 32-bit to 32-bit permutation, and DES S-boxes generate 4-bit quantities from 6-bit inputs. As discussed above, Adams specifically states that Adams' disclosed encryption methods do not employ DES S-boxes, and nowhere in Adams' disclosure is there a single mention of P-boxes or a combination of DES P-boxes and DES S-boxes to produce SP boxes. Adams simply does not teach that for which Adams was cited by the Examiner.

Additionally, in the 35 U.S.C. §102(b) anticipation rejection of claim 1, the Examiner states that Adams teaches "computing an index for each SP-box lookup table" on lines 51-67 of column 5. Lines 51-67 of column 5 are provided below, for the reader's convenience:

> Set the n vectors ϕ_i to be the columns of the matrix **M** representing the s-box. Check that **M** has $\mathbf{2}^m$ distinct rows and that the Hamming weight of each row and the Hamming distance between pairs of rows is close to n/2 (i.e., that the set of weights and the set of distances each have a mean of n/2 and some suitably small, but nonzero, variance). As well, if the i^{th} row of **M** is denoted by r_i, it should be verified that $(r_i \oplus r_j) \neq (i \oplus j)$ for any $i,j \in \{1, . . . ,2^m\}$, $i \neq j$ so that a non-zero input XOR is never equal to its resulting output XOR in the s-box (which may greatly facilitate finding a differential characteristic for the cipher). This latter condition will, in general, hold if the Hamming distance condition is met. If these conditions are not all satisfied, continue choosing suitable bent vectors (i.e. candidate ϕ_i) and checking the resulting matrix until the conditions are satisfied.

As can be quickly discerned by the reader, there is no mention in the above-quoted portion of Adams of SP-box lookup tables or indexes for SP-box lookup tables. As discussed above, Adams does not use DES S-boxes, P-boxes, or SP-boxes. The above-quoted portion of Adams discusses criteria for design of CAST-cipher S-boxes, which, as explicitly stated by Adams, are different from DES S-boxes. The above-quoted portion of Adams therefore does not disclose that for which it was cited by the Examiner.

The same above-quoted portion of Adams, lines 51-67 of column 5, are cited by the Examiner as teaching "computing the index for each SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES expansion permutation and said modified round key computation function." It is simply impossible for the above-quoted portion of Adams to teach computing the index for each SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES expansion permutation and any other value, because, as discussed above, the CAST-cipher-based encryption methods disclosed by Adams do not employ an expansion permutation operation. SP-boxes, DES expansion permutation operations, and the remaining portions of the step which the Examiner claims to be taught by the above-quoted portion of Adams are not once mentioned, suggested, or alluded to in the above-quoted portion of Adams. Please recall the DES expansion permutation step generates a 48-bit result from a 32-bit input. All of CAST S-box operations shown in Figure 2 of Adams are 32-bit operations.

Moreover, Adams does not teach, mention, or suggest any type of modification or transformation of the DES round function, or, as stated by the Examiner in paraphrasing claim 1, "adding operations to the DES round key computation function of obtain a modified round key computation function" because Adams does not employ the DES round function, instead employing a CAST-cipher-based round function that lacks all four steps of the DES round function described in the current application and in Menezes. In summary, Adams does not teach even a single one of the four steps of claim 1.

The rejections of independent claims 1, 2, 8, 17, and 19 all follow, in form, the rejection of claim 1, discussed above, and cite many of the same sections of Adams as cited in the rejection of claim 1. None of these rejections are justified or reasonable. Claim 1, and the other claims of the current application, are directed to an improvement of the DES data encryption standard encryption process, as discussed above, and as clearly claimed in each of the independent claims of the current application. For example, claim 1 claims a "method of reducing computation during each data encryption standard (DES) encryption and decryption round." Furthermore, the claims specifically mention DES round key computation functions, SP-boxes, and other DES-specific concepts and operations. Adams clearly, repeatedly, and explicitly states that Adams is directed to a non-DES CAST-cipher-based encryption method. This method, as clearly shown in Figures 1 and 2 of Adams, does not employ many of the DES steps and data structures. It also does not use DES S-boxes and P-boxes, and therefore cannot possibly use DES SP-boxes, which represent combinations of DES S-boxes and P-boxes.

As stated in MPEP § 2131, and in many different Federal circuit opinions:

> "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil CO. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Because Adams does not disclose, teach, or even mention the majority of the claim elements of the independent claims of the current application, and because Adams does not teach, mention, or even suggest an encryption method that employs the many DES operations and data structures explicitly mentioned in the independent claims of the current application, Adams cannot anticipate the independent claims of the current application.

In the Examiner's Response to Amendment section of the Office Action, the Examiner states that "the recitation 'a method of reducing computation during each data encryption standard encryption and decryption round' has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone." This is not, in Applicant's representative's respectfully offered opinion, a complete and correct statement of current Federal case law, or even of *Kropa v. Robie*. It has long been recognized by the Federal Courts that if the preamble of a claim is "necessary to give life, meaning, and a vitality" to the claim, then it should be construed as a claim limitation. See, e.g., *Kropa v. Robie*, 187 F. 2d 150, 152 (CCPA 1951). Indeed, in section 2111.02 of the MPEP, the MPEP states that:

> [a]ny terminology in the preamble that limits the structure of the claimed invention

> must be treated as a claim limitation. See e.g., *Corning Glass Works v. Sumitomo Elec. U.S.A., Inc.*, 868 F. 2d 1251, 1257, 9 USPQ 2d 1962, 1966 (Fed. Cir. 1989) (The determination of whether preamble recitations are structural limitations can be resolved only on review of the entirety of the application "to gain an understanding of what the inventors actually invented and intended to encompass by the claim.")

And yet another opinion states:

> Whether a preamble stating the purpose and context of the invention constitutes a limitation of the claimed process is determined on the facts of each case in light of the overall form of the claim, and the invention as described in the specification and illuminated in the prosecution history. *Applied Materials, Inc.* v. *Advanced Semiconductor Materials Am., Inc.*, 98 F.3d 1563, 1572-73, 40 USPQ2d 1481, 1488 (Fed. Cir. 1996).

The current claims contain many references to DES, encryption data structures, and operations. The preamble language reaffirms the fact that those DES-specific data structures and operations mentioned in the elements of the claim indeed describe DES-specific data structures and operations. Moreover, the preamble facilitates understanding that the current application is directed to improving the DES encryption method, as discussed above, by increasing computational efficiency of the DES encryption method. This, in turn, points to the fact that Adams' CAST-cipher-based technique, developed to increase the security of CAST-like ciphers with respect to differential and linear cryptanalysis, as discussed on lines 15-23 of column 5 of Adams, is directed to, and discloses, an encryption method quite different from the DES-encryption method developed under quite different motivations and assumptions. The current independent claims are directed to a more computationally efficient DES encryption method, as made clear both by the preambles of the current independent claims and by the specific mention of DES and DES-specific data structures and operations in the independent claims. The preamble language quite clearly indicates that, for example, the term "S-box" used in the current claims refers to a DES S-box, and not to a very different CAST-cipher S-box. The preamble language does, indeed, contribute to clarifying and defining the claim terms, and cannot, in Applicant's representative's respectfully offered opinion, be dismissed.

In section 5 of the Office Action, the Examiner states that Adams "teaches the limitations' language, and is explicit regarding the use of the modifications to improve the data encryption standard (columns 5-8)." Furthermore, the Examiner states that "Adams teaches enhancements to the round function of DES (columns 3-5) as does the claimed invention." As discussed above, these statements are incorrect. Adams explicitly states that

Adams uses CAST-like ciphers, rather than DES-ciphers, to construct a Feistel-structured SPN based on CAST ciphers. Adams' disclosed encryption method is not the DES encryption method, as clearly and unambiguously stated by Adams. The language "DES-like" initially used by Adams serves as a very strong indication that Adams' encryption method is not the DES encryption method, and that Adams' disclosure is likely inappropriate for an anticipation rejection. Comparison of Adams' Figures 1 and 2 to Figures 3 and 4 of the current application reveals that Adams' disclosed method cannot possibly anticipate an improved DES encryption method that employs a different SP-box indexing method and differently ordered SP-box lookup tables.

ISSUE 2

2. Whether claims 4 and 13 are unpatentable over Adams in further view of Candelor under 35 U.S.C. §103(a).

In rejecting claims 4 and 13, the Examiner states that Adams teaches the limitations as set forth under claims 3 and 12. As discussed above, Adams does not teach, disclose, mention, or suggest the computationally efficient DES encryption method of claims 4 and 13, or of the independent claims 2 and 11 from which claims 4 and 13 depend. Candelore is directed to an anti-tamper shield for an integrated circuit.

According to MPEP § 2143:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

Because Adams does not teach, mention, or suggest a DES encryption method, let alone the computationally efficient DES-encryption method to which the current claims are directed, and because Candelore is related to the current application at most by mentioning a DES hardware processor in a single sentence in column 6, with no mention of "computing a modified SP-box index" in order to improved the computational efficiency of the DES encryption, no combination of Adams and Candelore can possibly make any claim in the current application obvious.

ISSUE 3

3. Whether claims 5-7 and 14-16 are unpatentable over Adams in further view of Menezes et al. under 35 U.S.C. §103(a).

In rejecting claims 5-7 and 14-16, the Examiner states that "Adams teaches the limitations as set forth under claim" 2 and claim 11, and that "Adams and Menezes et al. teaches the limitations as set forth under" claim 5 and claim 14. Menezes teaches exactly the DES encoding method described in the Background of the Invention section current application, as discussed above. As discussed above, Adams does not teach, disclose, mention, or suggest the DES encryption method, but is instead directed to a different, CAST-cipher-based encryption method. Adams does not once mention P-boxes, SP-boxes, or the DES expansion permutation operation. According to MPEP § 2143:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

Because Adams does not teach, mention, or suggest a DES encryption method, let alone the computationally efficient DES-encryption method to which the current claims are directed, and because Menezes simply teaches the DES encryption method summarized in the Background of the Invention section of the current application, no combination of Adams and Menezes can possible make obvious any of the claims of the current application, all directed to a more computationally efficient DES encryption method in which a novel SP-box-indexing method is employed to eliminate the need for certain bit-reordering instructions needed to carry out standard DES encryption.

CONCLUSION

As discussed in detail, above, Adams does not teach, mention, or suggest a more computationally efficient DES encryption method, but instead discloses a different, CAST-cipher-based encryption method. Adams' disclosed encryption method does not employ P-boxes, SP-boxes, or the DES expansion permutation operation that are all explicitly recited in the current claims, and cannot possibly anticipate current claims directed to a more computationally efficient DES encryption method. Candalore makes a single reference to DES encryption processor, which presumably would carry out the standard DES encryption method. Candalore is therefore irrelevant to the currently claimed invention. Menezes reviews the standard DES encryption method, and, at best, therefore serves to confirm the teachings of the Background of the Invention section of the current application. No possible combination of Adams, Candalore, and/or Menezes can make obvious the currently claimed, more computationally efficient DES encryption method. None of the cited references are directed to improving the computational efficiency of DES, and none provide any teaching or suggestion for doing so.

Applicant respectfully submits that all statutory requirements are met and that the present application is allowable over all the references of record. Therefore, Applicant respectfully requests that the present application be passed to issue.

Respectfully submitted,
John Patrick McGregor, Jr.
OLYMPIC PATENT WORKS PLLC

By Robert W. Bergstrom
Robert W. Bergstrom
Reg. No. 39,906

Olympic Patent Works PLLC
P.O. Box 4277
Seattle, WA 98104
206.621.1933 telephone
206.621.5302 fax

CLAIMS APPENDIX

1. A method of reducing computation during each Data Encryption Standard (DES) encryption and decryption round, the method comprising the steps of:

a) generating at least one large SP-box lookup table;

b) computing an index for each SP-box lookup table;

c) adding operations to the DES round key computation function to obtain a modified round key computation function; and

d) computing the index for each SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function.

2. A method of reducing the number of software instructions required to perform permutation and substitution operations using Data Encryption Standard (DES) encryption and decryption rounds, wherein each round has a 64-bit input, and 32 bits of that 64-bit input are applied as the input to the DES Expansion Permutation, the method comprising the steps of:

a) generating at least one large SP-box lookup table;

b) adding operations to the DES round key computation function to obtain a modified round key computation function;

c) computing a modified SP-box index by performing XOR operations between at least one block of contiguous bits of the 32-bit input to the DES Expansion Permutation and the result of the modified round key computation function of step b); and

d) executing each subsequent round of DES computation by repeating steps a) and c).

3. The method recited in claim 2, wherein steps a) through d) are carried out in a digital processor.

4. The method recited in claim 3, wherein said digital processor is taken from the group consisting of a general-purpose processor, an embedded processor and a cryptographic processor.

5. The method recited in claim 2, wherein step c) comprises the step of selecting two blocks of contiguous bits of the 32-bit input to DES Expansion Permutation.

6. The method recited in claim 5, wherein one of said two blocks includes the least significant bit of said 32-bit input and the other of said two blocks includes the most significant bit of said 32-bit input for each of said round.

7. The method recited in claim 2, wherein step c) is carried out by permuting the entries within each SP-box lookup table.

8. In a processor carrying out a Data Encryption Standard (DES) computation by iterative DES rounds, a method of reducing computation associated with the DES Expansion Permutation by reducing the number of instructions required to compute the inputs to DES SP-boxes, the method comprising the steps of:

a) mathematically transforming the DES round function in each said round;

b) mathematically transforming the DES round key computation function in each said round; and

c) modifying the inputs to said SP-boxes in accordance with the results of steps a) and b).

9. The method recited in claim 8, wherein steps a) and b) are carried out so that computation in the DES Expansion Permutation is shifted from the DES round function to the DES round key computation function.

10. An apparatus for reducing computation during each Data Encryption Standard (DES) encryption and decryption round, the apparatus comprising:

a) means for generating at least one large SP-box lookup table;

b) means for computing an index for each SP-box lookup table;

c) means for adding operations to the DES round key computation function to obtain a modified round key computation function; and

d) means for computing the index for each said SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function.

11. An apparatus for reducing the number of software instructions required to perform permutation and substitution operations in the Data Encryption Standard (DES) encryption and decryption rounds, wherein each round has a 64-bit input and 32 bits of that 64-bit input are applied as the input to the DES Expansion Permutation, the apparatus comprising:

a) means for generating at least one large SP-box lookup table;

b) means for adding operations to the DES round key computation function to obtain a modified round key computation function; and

c) means for computing a modified SP-box index by performing XOR operations between at least one selected block of said 32-bit input to the DES Expansion Permutation and the result of the modified round key computation function.

12. The apparatus recited in claim 11, wherein said means for computing comprises a digital processor.

13. The apparatus recited in claim 12, wherein said digital processor is taken from the group consisting of a general-purpose processor, an embedded processor and a cryptographic processor.

14. The apparatus recited in claim 11, wherein said means for computing comprises means for selecting two blocks of said 32-bit input to the DES Expansion Permutation.

15. The apparatus recited in claim 14, wherein one of said two blocks includes the least significant bit of said 32-bit input and the other of said two blocks includes the most significant bit of said 32-bit input for each of said round.

16. The apparatus recited in claim 11, wherein said means for generating comprises means for permuting the entries within each said SP-box lookup table.

17. In a processor carrying out a Data Encryption Standard (DES) computation by iterative DES rounds, an apparatus for reducing computation associated with the DES Expansion Permutation by reducing the number of instructions required to compute the inputs

to DES SP-boxes, the apparatus comprising:

a) means for mathematically transforming the DES round function in each said round;

b) means for mathematically transforming the DES round key computation function in each said round; and

c) means for modifying the inputs to said SP-boxes in accordance with the transformations of said round function and of said round key computation function.

18. The apparatus recited in claim 17, wherein means for modifying comprises means for shifting computation in the DES Expansion Permutation from the DES round function to the DES round key computation function.

19. A data processing system for carrying out Data Encryption Standard (DES) encryption and decryption rounds with reduced computation, the system comprising:

a) computer processing means for processing data;

b) storage means providing four large SP-box lookup tables;

c) means for computing indices for the respective SP-box lookup tables;

d) means for adding operations to the DES round key computation function to obtain a modified round key computation function; and

e) means for computing the index of each said SP-box by performing XOR operations between at least one block of contiguous bits of the input to the DES Expansion Permutation and said modified round key computation function.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.